DNS over CoAP (DoC) &
Discovery of Network-designated CoRE Resolvers

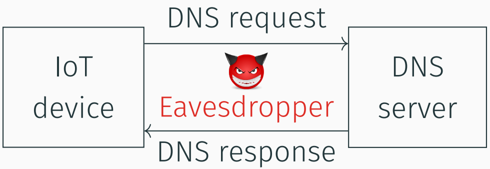
`draft-ietf-core-dns-over-coap`
`draft-lenders-core-dnr`

Martine S. Lenders (martine.lenders@tu-dresden.de), Christian Amsüss, Cenk Gündoğan, Thomas C. Schmidt, Matthias Wählisch

IETF 119, CoRE WG Session, 2024-03-20

Motivation for DNS over CoAP

Attack Scenario



Countermeasure: Encrypt name resolution triggered by IoT devices against eavesdropping

Our Proposal: DNS over CoAP (DoC), `draft-ietf-core-dns-over-coap`

- **Encrypted communication** based on DTLS or OSCORE
- **Block-wise message transfer** to overcome Path MTU problem (DNS over DTLS)
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism

Changes to DoC Draft

Since IETF 118

+ Add references to relevant SVCB/DNR RFCs and drafts

Deliverables from IETF 118 for WGLC

- Implementations
  - ✓ Python/aiocoap server
  - ✓ RIOT/gCoAP client
  - ✓ WIP: Implementation in Unbound
  - ? More?
- Problem Statement regarding Service Bindings
  - ✓ Discovery of Network-designated CoRE Resolvers
    ⇒ draft-lenders-core-dnr

Resolver Discovery (I)

Current landscape:

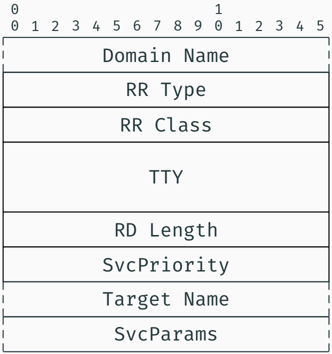
- Discovery of Designated Resolvers (DDR), RFC 9462
  - Uses SVCB Record definitions from RFCs 9460 and 9461
- DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR), RFC 9463
  - Puts SvcParams from RFC 9460 and 9461 into DHCP and RA options

Resolver Discovery (II)

DDR

DNS SVCB Resource Record

(RFCs 9460, 9461, 9462)

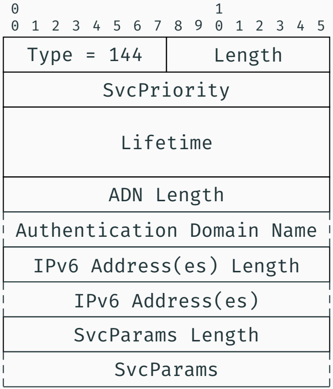


```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-------------------------------+
|          Domain Name          |
+-------------------------------+
|            RR Type            |
+-------------------------------+
|           RR Class            |
+-------------------------------+
|                               |
|              TTY              |
|                               |
+-------------------------------+
|           RD Length           |
+-------------------------------+
|          SvcPriority          |
+-------------------------------+
|          Target Name          |
+-------------------------------+
|           SvcParams           |
+-------------------------------+
```

DNR

IPv6 RA Option

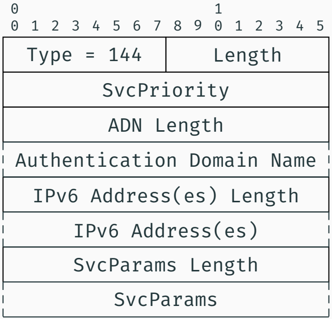
(RFC 9463)



```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---------------+---------------+
|  Type = 144   |    Length     |
+---------------+---------------+
|          SvcPriority          |
+-------------------------------+
|                               |
|           Lifetime            |
|                               |
+-------------------------------+
|          ADN Length           |
+-------------------------------+
| Authentication Domain Name    |
+-------------------------------+
|   IPv6 Address(es) Length     |
+-------------------------------+
|       IPv6 Address(es)        |
+-------------------------------+
|       SvcParams Length        |
+-------------------------------+
|           SvcParams           |
+-------------------------------+
```

DHCPv6 Option

[DHCPv4 Option comparable]
(RFC 9463)



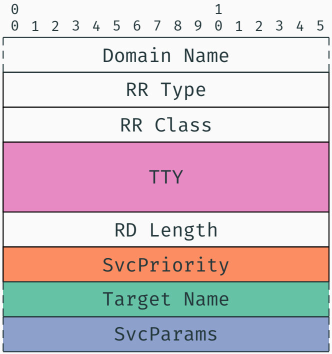
```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---------------+---------------+
|  Type = 144   |    Length     |
+---------------+---------------+
|          SvcPriority          |
+-------------------------------+
|          ADN Length           |
+-------------------------------+
| Authentication Domain Name    |
+-------------------------------+
|   IPv6 Address(es) Length     |
+-------------------------------+
|       IPv6 Address(es)        |
+-------------------------------+
|       SvcParams Length        |
+-------------------------------+
|           SvcParams           |
+-------------------------------+
```

Resolver Discovery (II)

DDR

DNS SVCB Resource Record

(RFCs 9460, 9461, 9462)



```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
```

Domain Name

RR Type

RR Class

TTY

RD Length

SvcPriority

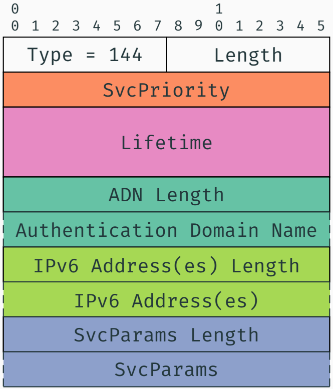
Target Name

SvcParams

DNR

IPv6 RA Option

(RFC 9463)



```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
```

Type = 144 | Length

SvcPriority

Lifetime

ADN Length

Authentication Domain Name

IPv6 Address(es) Length

IPv6 Address(es)

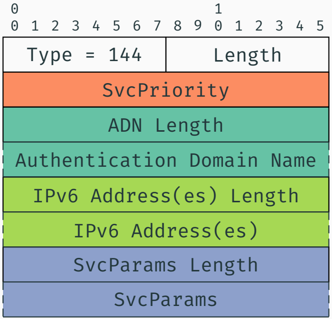
SvcParams Length

SvcParams

DHCPv6 Option

[DHCPv4 Option comparable]

(RFC 9463)



```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
```

Type = 144 | Length

SvcPriority

ADN Length

Authentication Domain Name

IPv6 Address(es) Length

IPv6 Address(es)

SvcParams Length

SvcParams

Resolver Discovery (II)

DDR

DNS SVCB Resource Record

(RFCs 9460, 9461, 9462)

DNR

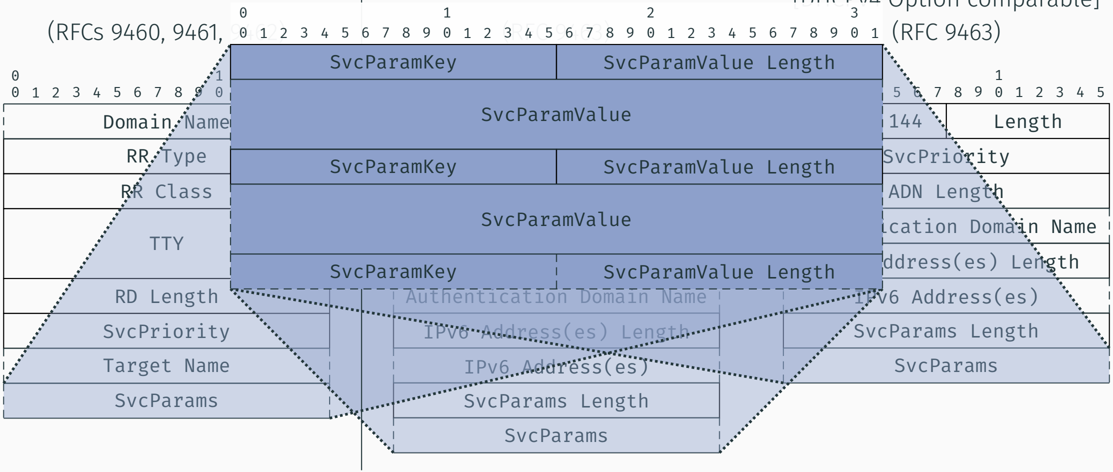
IPv6 RA Option

(RFC 9463)

DHCPv6 Option

[DHCPv4 Option comparable]

(RFC 9463)



Domain Name

RR Type

RR Class

TTY

RD Length

SvcPriority

Target Name

SvcParams

Authentication Domain Name

IPv6 Address(es) Length

IPv6 Address(es)

SvcParams Length

SvcParams

144

Length

SvcPriority

ADN Length

…cation Domain Name

…ddress(es) Length

IPv6 Address(es)

SvcParams Length

SvcParams

SvcParamKey | SvcParamValue Length

SvcParamValue

SvcParamKey | SvcParamValue Length

SvcParamValue

SvcParamKey | SvcParamValue Length

What are the Problems with Resolver Discovery for CoAP?

- **SvcParamKeys/SvcParamValues missing?**
  - `alpn="coap"` exists for CoAP over TLS
  - `alpn="co"` registered by `draft-lenders-core-dnr` for CoAP over DTLS
  - CoAP transfer protocol beyond TLS/DTLS (UDP, TCP, GATT, …)? `coaptransfer` (see also `draft-ietf-core-transport-indication`)
  - OSCORE? ACE? `objectsecurity`, `oauth-...`
  - Equivalent to `dohpath`: Early allocation request for `docpath`?
- **What should Authenticator Domain Name/Target Name be for OSCORE?**
  - Empty if no name to authenticate?
  - Future-proofing for CA-style authentication with EDHOC?

Easily solvable problems ⇒ We solved most of them in `draft-lenders-core-dnr`

Feedback welcome from OSCORE/EDHOC experts!

Is `draft-ietf-core-dns-over-coap` ready for

WGLC?